REMARKS/ARGUMENTS

Prior Asserted Rejections under 35 U.S.C. § 112

Claims 19 and 20

The Examiner says that "the signal quality level" that is referenced in Claim 19 is indefinite because there is no previous introduction of the term "signal quality level." It is submitted that the term "the signal quality level" is not indefinite because one of ordinary skill in the art would read the term as referring to the degradation levels of the first level degraded data signal and the second level degraded signal—which are clearly discussed in Claim 14. The following amendment to Claim 19 is offered as per the Examiner's suggestion-- "... the data signal quality levels...". Accordingly, it is requested that this rejection be withdrawn.

With respect to the 112 rejection of Claim 20, it is submitted that the term "the predetermined signal quality level" is not indefinite because one of ordinary skill in the art would read the term as referring to the degredation levels of the first level degraded data signal and the second level degraded signal—which are clearly discussed in Claim 14. The following amendment to Claim 20 is offered as per the Examiner's suggestion-- "... predetermined data signal quality level..." Accordingly, it is requested that this rejection be withdrawn.

Rejections under 35 U.S.C. § 102

§ 102 Rejections based on Hirose

Claims 1-8, 12-20, 60, 62, 63, 66-68 stand rejected as allegedly anticipated by U.S. Patent No. 5,917,915 issued to Hirose (hereafter "Hirose"). See Page 3 of the September 30, 2004 Office Action.

Claim 1 (and all claims depending therefrom) and Claim 66 (and all claims depending therefrom)

In order for a reference to anticipate a claim, the reference must disclose each and every limitation of the claimed invention, either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation. *See Atlas Powder Co. v. Ireco Inc.*, 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1947 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994). Independent Claim 1 recites, *inter alia*, "A method for securing a data object, comprising: providing a data object comprising digital data and file format information; embedding independent data into the data object; and scrambling the data object to degrade the data object to a predetermined signal quality level. The 102 rejection based on Hirose is improper for at least the reason that Hirose fails to disclose (1) "embedding independent data" and (2) "scrambling the data object to degrade the data object to a predetermined signal quality level" as required by the rejected claims. The 102 rejection is similarly flawed for Claim 66 (and all dependent claims), as Hirose does not disclose (1) an "embedder" and (2) a "scrambler" as required by the claim limitations.

Further, regarding Claim 1 and 66, the Examiner asserts that "... Hirose teaches a method/system for securing a data object comprising: providing a data object comprising digital data and file format information (col. 4, lines 51-55 and col. 5, lines 4-13); embedding independent data into the data object (fig. 3, ref. num 12); and scrambling the data object to degrade the object to a predetermined signal quality level (fig. 2, ref. num 27 and col. 5, lines 14-34)," September 30, 2004 Office Action at Page 3. The Examiner's assertion is unsupported by Hirose. First, Hirose does not teach, "embedding independent data"-- at any point. Instead, Hirose appears to disclose an invention for encrypting content for broadcast, not "securing data within the data objects", as per the Applicants' claimed invention[s]. For this reason alone, the 102 rejection is improper. Encrypting "data" actually teaches away from "embedding", "scrambling", or combinations of the techniques, as per the Applicants' claim language. The encrypted data is *de facto* inaccessible. In fact, Hirose requires that users first pay or subscribe to data *prior to receiving it*. This teaches away from making the "data objects" of the Applicants accessible for evaluation and potentially, subsequent purchase, albeit in a scrambled or degraded state. For this additional reason the 102 rejection should be withdrawn. Hirose discloses at Col. 2 ll. 5-15, data is encrypted and requires a decryption key to be decrypted:

> In the above-described scramble system, a scramble key is required to decrypt the scrambled program when the scrambled

> program is received. As a consequence, for instance, if the newspaper data (namely, scrambled newspaper data) have been received prior to the establishment of a contract are recorded on the recording medium, after the establishment of the contract, even if the contractor may have his own scramble key, he cannot decrypt the scrambled newspaper data which have been recorded on this recording medium.

Hirose discusses this approach in the same context at Col. 1 ll. 33-38 and Col. 2 ll. 41-48, as well. Hirose's "data" is not "scrambling the data object to degrade the data object to a predetermined signal quality level", as required by the claimed invention[s], and could not logically be scrambled this way since he encrypts the categorized "data" twice— and, as disclosed above, sometimes leaving the "contractor" of the data without a means for decryption. See Hirose at Col. 2 line 52 – Col. 31 line 15.

The Examiner cites Figure 2 & Figure 3, as allegedly having application to Applicant's securing "data objects". However, Figure 2 clearly applies a scrambler for encryption, not scrambling to produce a "degraded data signal" as required by the claim[s]. In fact, by requiring that the data be encrypted twice, the data cannot be observed in lower quality versions or made accessible to retrieving the embedded "independent data". It is not possible to detect or decode "embedded independent data" from encrypted data. Figure 3 Ref. Num 12 is a multiplexer used to *associate* information with encrypted data being transferred—no identification could be made of the data once encrypted, as required by Hirose. Hirose at Col. 6 ll. 5-17:

> The transfer channel scramble key, the common information, the receiver apparatus ID and the contents of the contracts are supplied to an encrypt circuit 11 (the transfer channel scramble key is also supplied to the PN generator 13) so as to be encrypted. The encrypted data is supplied as relevant information to the independent data channel multiplexing circuit 12.
>
> The independent data channel multiplexing circuit 12 multiplexes the scrambled newspaper data supplied from the data scrambler 14 with the relevant information supplied from the encrypt circuit 11, and the multiplexed data is outputted therefrom to a digital channel signal multiplexing circuit 15.

This separation teaches away from the Applicants' invention and claim language for at least the reason that Hirose teaches encryption, there is no "embedding of independent data" and no "scrambling ... to a predetermined signal quality level". Applicants teach that open access to data objects at degraded "predetermined signal quality level[s]" is likely to induce purchasing of the original data object (which has not been degraded). Hirose teaches encryption, where, absent a contract for purchase, prevents decryption of or access to the data. Hirose at Col. 11 ll. 63 – Col. 12 ll. 6:

> Nevertheless, as previously stated, since when the newspaper (program) data is received, the scramble key (information unit scramble key) is required so as to descramble this scrambled (partially scrambled) newspaper data, if the information unit scramble key is transmitted via the satellite 4, then this information unit scramble key cannot be received before making the contract. As a consequence, such information 2 which has been received and recorded on the recording medium 8 before establishing the contract cannot be descrambled after the contract is made.

The Examiner's further assertion that Hirose discloses "embedding independent data" is unsupported. There is no teaching of "embedding independent data" nor would it be apparently necessary since Hirose associates (e.g., does not embed) identification and decryption keys with encrypted transferred data, thereby teaching away from Applicants' claimed invention[s].

As for Hirose's alleged teaching of "scrambling the data object to degrade the object to a predetermined signal quality level", September 30, 2004 Office Action at Page 3, no such method or system is taught. Hirose does teach that separate categories of newspaper data maybe segmented by encryption keys; see Hirose at Col. 5 ll. 14-62. But, Hirose does not teach "embedding independent data" and "scrambling" "data objects", let alone "embedding" and "scrambling" of Hirose's disclosed "data", at predetermined signal quality levels to entice purchases or otherwise enable various methods for authentication, payment, and allocation of bandwidth as per Applicants' invention[s].

Because Hirose fails to disclose (1) "embedding independent data into a data object" and (2) "scrambling the data object to degrade the data object to a predetermined signal quality level" as required by Claim 1, the Section 102 rejection of Claim 1 must be withdrawn. Similarly, Hirose fails to disclose (1) an "embedder" and (2) a "scrambler" as required by Claim 66. Moreover, for the same reasons that Claim 1 and Claim 66 are patentable over Hirose, the claims that depend from Claim 1 and Claim 66 are also patentable. Applicants request the Examiner withdraw the Section 102 rejections of Claims 1 and 66 and all claims depending therefrom based on Hirose.

Claims 2, 3, 5 and 6

Applicants respectfully disagree with the Examiner's assertions that "... Hirose teaches the step of performing the steps of embedding and scrambling until a predetermined condition is met (col. 5, lines 14-23)" and "... Hirose teaches the predetermined condition comprises reaching a desired signal quality level of the data object (col. 5, lines 35-39)", September 30, 2004 Office Action at Page 3. Hirose teaches encryption of data to prevent unauthorized access, see arguments above. For these reasons, Hirose does not teach "embedding" and "scrambling", let alone "... the step of performing the steps of embedding and scrambling until a predetermined condition is met" as required by the claim limitations— encryption prevents this *de facto*. The Examiner apparently fails to identify any "predetermined condition" that must be met before any

"embedding" and "scrambling" process is stopped. The Examiner has failed to establish a case of anticipation. Applicants therefore request the Examiner to withdraw the Section 102 rejections for Claims 2, 3, 5 and 6 based on Hirose.

Claims 4 and 67

Applicants respectfully disagree with the Examiner's assertion that "... Hirose teaches the steps of: [d]escrambling the data object to upgrade the data object to a predetermined signal quality level (fig. 6, ref. num 31 and col. 9, lines 29-42); and [d]ecoding the embedded independent data (col. 9, lines 21-27)", September 30, 2004 Office Action at Page 3, it is not logical to assert that Hirose teaches "descrambling" and "decoding embedded independent data" since Hirose does not teach "embedding" and "scrambling" in the first place. Hirose, at Col. 9 ll. 21-42, is a reiteration of decryption of Hirose's contracted and encrypted newspaper data. That Hirose is directed at encryption of data (e.g. Figure 12 in addition to previously cited sections in Hirose) is antithetical to the teaching of "embedding" and "scrambling" to assist with enticing consumers to buy after listening or viewing content in an "embedded" and "scrambled", e.g. degraded, state. This initial purchase is made after listening or viewing a degraded signal and thus not the encrypted content of Hirose. Nor, is any mention of "embedding" provided in Hirose to assist with determination of consumer demand, authentication, payment, and bandwidth allocation as argued by the Applicants. Applicants therefore request the Examiner to withdraw the Section 102 rejections for Claims 4 and 67 based on Hirose.

Claim 13

Applicants respectfully disagree with the Examiner's assertion that "... Hirose teaches the step of scrambling the independent data before the embedding step so that the embedding step embeds the scrambled independent data into the data object (fig. 3, ref. num 11 comes before 12)" September 30, 2004 Office Action at Page 4. As argued previously, Hirose apparently teaches associating authorization information (e.g., pre-existing subscribers) with his encrypted data, Hirose at Col. 3 ll. 2-14. However, Hirose asserts that the authorization is prior to the content being transferred—the subscribers are "pre-existing". Associating identification information with "encrypted data" is not equivalent with "embedding independent data" into a "data object". Moreover, Hirose does not teach "scrambling" of any "independent data" prior to an encoding step. No "embedding" or "scrambling" is disclosed. Claim 13 additionally requires "scrambling the independent data before the embedding step so that the embedding step embeds the scrambled independent data into the data object." Hirose fails to disclose this claim limitation. Applicants therefore request the Examiner to withdraw the Section 102 rejection for Claim 13 based on Hirose.

Claims 14 and 68

Applicants respectfully disagree with the Examiner's assertion that "... Hirose teaches a method/system for distributing a data signal comprising ... [s]electing a first scrambling technique to apply to the data signal (col. 5, lines 14-24); scrambling the data signal ... resulting in a first level degraded data signal (col. 5, lines 14-24) ... scrambling

the first-level degraded data signal using a second scrambling technique, resulting in a second-level degraded data signal (col. 5, lines 52-62); and, creating a second descrambling key for the second-level degraded signal based on the second scrambling technique (col. 9 , lines 8-13)" September 30, 2004 Office Action at Pages 4 and 5. The 102 rejection is improper for at least the reason that Hirose fails to disclose (1) "a first-level degraded signal" or (2) "a second-level degraded data signal". Since Hirose encrypts his "newspaper data", described in Figure 2, it is not possible to apply a (1) "second scrambling technique to apply to the first-level degraded data signal" and (2) "scrambling the first-level degraded data signal using a second scrambling technique, resulting in a second-level degraded data signal". For these additional reasons the 102 rejection must be withdrawn.

Similarly, Claim 68 requires (1) "a first-level degraded signal" and (2) "a second-level degraded data signal". Scrambling of the data signal in tiers, as per the claim language, requires logically separate scramblers—one for (1) "a first scrambler" and one for (2) "a second scrambler". That Hirose encrypts his "newspaper data" results in unobservable data, not information which has been degraded at least twice, as per the Applicants' claim limitation[s]. In fact, the manner in which Hirose's data must be "decrypted" requires at least two encryption keys; but, one of these keys is directed at the "transfer channel" not the data signal itself, thus, making obvious that Hirose teaches away from scrambling data signals in a tiered manner. Further, each piece of "newspaper data" described by Hirose is separately encrypted. Hirose at Col. 10 ll. 35-38 [emphasis added]: "On the other hand, **another receiver (contractor) who can receive *both* of the transfer channel scramble key and the information unit scramble key can observe the entire newspaper.**" Hirose is clearly separating the encryption of the "information units" from the channel for which the "information units" are transferred. As argued above, the "transfer channel scramble key" of Hirose is not directed at the "data" but at the channel for which "information units" may be transferred. The data is not degraded it is not even "observable" as disclosed by Hirose. For these additional reasons the Applicants request the Examiner to withdraw the Section 102 rejections for Claims 14 and 68 and all claims depending therefrom based on Hirose.

Claim 60

Applicants respectfully disagree with the Examiner's assertion that "... Hirose teaches a method for bandwidth allocation, comprising: presenting a plurality of data objects to a user ... linking at least a first data object to at least one second data object (fig. 8); wherein a characteristic of the first data object causes a change in the second data object (col. 11, lines 13-37)" September 30, 2004 Office Action at Page 6. The 102 rejection is improper for at least the reason that Hirose fails to disclose (1) "linking at least a first data object to at least one second data object" or (2) "wherein a characteristic of the first data object causes a change in the second data object". Hirose alleges teaches a means for encrypting "newspaper data" for broadcast. The approach encrypts the data, making it unobservable, and encrypts the "transfer channel", independent of the data. Hirose never mentions any linking of data objects for "bandwidth allocation", nor a means for one data object to cause a change in a separate data object. In fact, Hirose teaches away from the Applicants' claimed invention[s] by requiring that at least one "newspaper data" be encrypted separately from other "newspaper data".

Hirose discloses the separateness of his "newspaper data" at Figure 7, and discusses the "broadcasting system" at Col. 9 l. 43 – Col. 10 l. 38. Hirose elaborates that under his scheme separate data objects are not "linked" nor does "a characteristic of the first data object causes a change in the second data object", as required by the claim[s]. For these additional reasons the 102 reject should be withdrawn. Hirose does direct that a receiver "... can make such a contract that either the entire newspaper data of this one newspaper, or the newspaper data excluding the commercial page and the local page can be received", Hirose at Col. 11 ll. 9-12. This departure from the Applicants' claimed invention[s] teaches away from enabling open access to a plurality of data objects where said objects may be linked and bandwidth may be effectively allocated based on said linking. Hirose clearly requires that each individually encrypted "information unit" be pre-paid and separately "broadcast". For these reasons the Applicants request the Examiner to withdraw the Section 102 rejections for Claim 60 and all claims depending therefrom based on Hirose.

Rejections under 35 U.S.C. § 103

In order to "establish a prima facie case of obviousness, three basic criteria must be met." MPEP § 7.06.02(j). First, there must be some motivation or suggestion to modify the reference or to make the proposed combination. Second, there must be a reasonable expectation of success. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure." MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Third, the combined references must teach or suggest all claim limitations.

The Examiner has failed to establish a *prima facie* case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. According to the MPEP,

> [i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner *must present a convincing line of reasoning* as to why the artisan would have found the claimed invention obvious in light of the teachings of the references.

MPEP 2142 (citing *Ex parte Clapp*, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)) [emphasis added]. Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing *Ex Parte Skinner*, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motivation to combine in *Winner Int'l Royalty Corp. v. Ching-Rong Wang*, 202 F. 3d 1340, 1348-49 (Fed. Cir. Jan. 27, 2000). "Although a reference need not expressly teach

that the disclosure contained therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be '**clear and particular**.'" *Winner*, 202 F. 3d at 1348-49 (citations omitted). Further, the "absence of such a suggestion to combine is *dispositive* in an obviousness determination." *Gambro Lundia AB v. Baxter Healthcare Corp.*, 11 F.3d 1573, 1579 (Fed. Cir. 1997) [emphasis added].

Applicants submit that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine for any of the proposed combinations of references. More significantly, the references, even in combination, do not disclose all elements of the Applicants' claimed invention[s].

§ 103 Rejections based on Hirose further in view of Wasilewski et al.

Claims 9-11, 21-23, 27-42, 44, 48, 49, 51-59, 64, and 65 have been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hirose (U.S. Patent No. 5,917,915) in view of Wasilewski et al. (U.S. Patent No. 5,870,474). Examiner asserts that " ... Hirose teaches all the limitations of claim 1, above," September 30, 2004 Office Action at Page 7. This assertion is unsupported. Hirose as disclosed earlier teaches encryption of data for the reasons discussed above. This teaches away from the present invention. Also, as discussed above, Hirose neither mentions nor discloses any form of "embedding" or "scrambling ... to a predetermined signal quality level".

First, the combination fails to disclose all of the elements of independent Claims 1, 21, 31, and 49 and all claims that depend therefrom, including Claims 14-20. That neither reference mentions "embedding", "encoding independent authentication data into the data object", "steganographic technique" or "scrambling ... to a predetermined signal quality level", the references cannot yield the claimed inventions of the Applicants even in combination. The Applicants Specification discusses limitations to proposed "copy protection" schemes, including blanket application of encryption, digital rights management, and the like, to the distribution of the content. Wasilewski et al. describes "conditional access" not "open access" in any form. Asserting that Hirose includes "copy protection" does not equate with the necessary claim element of embedding independent data into a data object. Nonetheless, the combination of the two does not disclose all of the elements of the claimed invention[s].

Second, it is unclear that the Examiner's reliance on assertions that "some form of copy protection would be desirable" relates to the Applicants' claimed inventions of providing open access to data objects. Applicants maintain that copying of "data objects" will happen. By offering accessible data objects that are scrambled with transfer functions at predetermined signal quality levels, unlike the teachings of Wasilewski et al. to *restrict access*, choices over how much improved quality (even quantity) can be made by the consumer. As the signal quality improves, more embedded independent data is recovered. The property of robustness taught by the Applicants refers specifically to resistance against signal manipulations, contrary to the Examiner's own definition. Thus, the Applicants respectfully request further explanations/support (for example, other citations or an affidavit if based on personal knowledge) for the Examiner's assertions that a "robust open watermark" has the following properties: "easy to be seen by any person wishing to access

the data"; "robust, the person will find it very difficult to remove the watermarking feature if the person were to choose to cheat the copyright holder"; and, "[t]he combination of a robust open watermark provides an easy to acknowledge, but very difficult to break, method of protecting copy written data", September 30, 2004 Office Action at Page 7, 8 and 10. It is unclear to the Applicants where these assertions originate, as they do not appear to be correctly supported in the art or by the Applicants Specification or claims. There are trade-offs between robustness, signal quality, and security in digital watermarking schemes in the art, and the Examiner appears to contradict these trade-offs.

Third, there is no motivation to combine Hirose with Wasilewski et al. Neither discloses any form of embedding or scrambling as per the Applicants' disclosure, and each appears to apply encryption in a manner as to require prior authorization to gain access to data. No data is presented with open access. Where is the motivation to combine? Each reference, even in combination, teaches away from embedding independent information and subsequently scrambling to predetermined signal quality levels. For at least these reasons Applicants respectfully request the Section 103 rejections to be withdrawn.

Claim 21

The Applicants respectfully disagree with the Examiner's assertions that Hirose in combination with Wasilewski et al. anticipates Claim 21 and the claims that depend therefrom. The Examiner incorrectly asserts that Hirose's method comprises: "... [p]roviding a data object comprising digital data and file format information (col. 4, lines 51-55 and col. 5, lines 4-13); and, manipulating the file format information based on at least one signal characteristic of the data object (col. 5, lines 58-65)," September 30, 2004 Office Action at Page 9. Hirose at Col. 4, ll 51-55 and Col. 5, ll 4-13, does not disclose digital data and file format information that can be "manipulated" as per the claim limitation. Hirose at Col. 4 ll. 51-55 addresses "newspaper data" being "edited"; and, the Col. 5 ll. 4-13 reference regards "newspaper data" being broken down into categories prior to being stored. Hirose, at Col. 5 ll. 58-65, discloses that the "scrambled newspaper data" is encrypted a second time *not* "encoding independent authentication data into the data object" and "manipulating the file format information based on at least one signal characteristic of the data object", as required by the claim, prior to "distributing a data object". Because Wasilewski et al. teaches conditional access by "encapsulating" content in encryption, "manipulating the file format information based on at least one signal characteristic of the data object", is *not* possible. Figure 3 explicitly recites three layers of encryption preventing access to the data object, teaching away from the claimed invention, Wasilewski et al. at Col. 7 l. 64 – Col. 8 l. 7:

> FIG. 3 presents a functional diagram of the presently preferred conditional access model. The present invention provides three functional levels of protection: (1) program encryption, (2) control word encryption and authentication, and (3) entitlement message encryption and authentication. At the first level, the program bearing MPEG-2 transport packets are encrypted using random number generated keys, referred to hereinafter

> as control words. At the second level, the control words are encrypted using a second randomly generated key. This second key is referred to hereinafter as a multi-session key (MSK). At the third level, the multi-session key is encrypted using a public key cryptography technique.

The Applicants' invention offers improvements over handling content by providing *open access* while including data object specific tracking, authentication, payment, and bandwidth allocation based on the step of "encoding independent authentication data". Thus, the combination of Hirose and Wasilewski et al. fails to disclose all of the elements of the Claim 21. For at least these reasons and the reasons previously argued above in connection with Claims 1, 31, and 49, Hirose, in combination with Wasilewski et al., does not yield the elements of the claimed invention; thus, the 103 rejection must be withdrawn.

Claims 31 and 49

The Applicants respectfully disagree with the Examiner's assertions that Hirose in combination with Wasilewski et al. anticipates Claim 31 and the claims that depend therefrom. The conditional access schemes of Wasilewski et al. depend on the devices not the "data objects" for enabling access. Wasilewski et al. does not allow "(1) embedding independent data into a data object; (2) scrambling the data object; (3) distributing the scrambled data object; (4) distributing at least one predetermined key that enables access to the data object; and, (5) descrambling the scrambled data object with the predetermined key". Wasilewski et al. at Figure 3 discloses that what is distributed is "MPEG-2 WITH CONDITIONAL ACCESS", Wasilewski et al. Figure 3 ref. 152. The three levels of encryption in Figure 3 rely on a third party authority, what is called a "conditional access authority" by Wasilewski et al. at Col. 22 ll. 49-60:

> Each STU 90 has a public key/private key pair. The private key is secured within the STU 90 in a secure processor. The associated public key is then published in a public key database server maintained by a conditional access authority 400. When an SP 110 wishes to provide conditional access to its programming for a particular STU 90, the CAM 30 looks up the public key for the STU 90 and sends the MSK to the STU 90 encrypted with the public key of that STU 90. The STU 90 can then decrypt the MSK using its corresponding private key. The CAM 30 maintains a data base of valid STU 90 public keys, which it periodically updates from the conditional access authority 400.

Wasilewski et al. thus teaches away from "descrambling the scrambled data object with the predetermined key" to improve signal quality and determine how the recovered, embedded "independent data" is utilized, relying instead on a "conditional access authority". Wasilewski et al.'s "public key/private key pair" is specific to the "STU" (set-top box), not the "data object" of the Applicants. For arguments sake, Wasilewski et al. would need one STU per "data object" to make each object unique, but would still not present the programming

in predetermined signal quality levels, for a given data object, that are embedded with independent data so that a consumer was able to "click through" to higher predetermined signal quality levels. Claim 31's dependent claims are directed at these novel features.

The combination of Hirose with Wasilewski et al. fails to disclose the claim limitations of Claim 31. Encryption and traditional digital signatures, as is known in the art and taught by Wasilewski et al., can easily be stripped from programming content without any price paid on the quality of the content. Digital watermarking is directed at causing signal degradation when attempts are made at erasure of the embedded data as well as causing nonauthentication of the embedded signal. Wasilewski et al. could not prevent differencing of "encrypted" with "decrypted" "programming" by the consumer to construct a set-top box (i.e., the decrypted data is in the clear at the consumer's set-top box). The Applicants' invention would not suffer such systemic attacks since the data objects are individually prepared by "embedding" and "scrambling", as argued previously. The benefits of "descrambling the scrambled data object with the predetermined key", a required claim element of Claim 31, enables authentication, payment measurement, measurements of bandwidth allocation and signal quality parameters. Hirose or Wasilewski et al., even in combination, clearly fail to disclose all of the claim elements. For these additional reasons the Section 103 rejections must be withdrawn from Claim 31 and the claims that depend therefrom.

Next, the combination of Hirose with Wasilewski et al. fails to disclose the claim limitations of Claim 49. Hirose teaches a means of encrypting data twice, as discussed previously. The data is encrypted when stored onto media, as discussed above. That being said, it would not be possible to "apply a steganographic technique for embedding independent data into the data signal", as required by independent claim 49, since the data signal is encrypted. Wasilewski et al. relies on content being separately stored in an encrypted state, neither data signal *is accessible* even after recording to a media, so it is illogical to conclude that one, let alone two or more scrambling states for a single data signal would be openly accessible. The Applicants' claimed inventions represent improvements over managing access to the contents of Hirose, Wasilewski et al. or combinations of both, by enabling consumers to determine the level of quality and making measurements of the data object more discrete based on manipulations of the data objects' signal characteristics or payment thresholds that can be associated with such signal manipulations, as presented in the dependent claims. Hirose, Wasilewski et al., even in combination, fail to disclose all of the claim elements. For at least these reasons, Section 103 rejections must be withdrawn from Claim 49 and the claims that depend therefrom.

§ 103 Rejections based on Hirose in view of Wasilewski et al. in further view of Allen

Claims 24-26, 43, 45-47, and 50 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hirose (U.S. Patent No. 5,917,915) in view of Wasilewski et al. (U.S. Patent No. 5,870,474) further in view of Allen (U.S. Patent No. 5,418,713). Examiner asserts that " ... the combination of Hirose in view of Wasilewski et al. teaches all of the limitations of claims 21, 31, and 49, respectively, above. However, the combination of Hirose in view of Wasilewski et al. does not teach the limitations of the following claims ...

24, 25-26, 43, 45-47, and 50," September 30, 2004 Office Action at Pages 18-21. This assertion is unsupported. For at least the reasons discussed above, neither Hirose, nor Wasilewski et al., even in combination discloses "embedding" or "scrambling" as required by the applicants' claim limitations. Combining with Allen fails to disclose the additional claim elements of dependent claims 24-26, 43, 45-47, and 50 and all claims that depend therefrom. Allen neither mentions nor discloses any form of "embedding" or "scrambling". Allen teaches "duplication" of "original content." This teaches away from the present invention. In fact, Allen discloses in the Abstract [emphasis added]:

> The central host server is connected to a communications network for communication to a remote server which controls a manufacturing control device connected thereto. The **manufacturing control device duplicates original content recordings on blank media upon receipt of a data representation of the original content recording from the remote server** which retrieves said data representation for a selected original content recording from the central host server over the communications network.

Further, Allen at Figure 7, does not disclose digital data and file format information that can be "manipulated" as per the independent claims from which these dependent claim. Allen at Col. 5 ll. 61-63, discloses that the "original content" may be "... mathematically resampled and digitally compressed during content capture..." *not* "encoding independent authentication data into the data object" and "manipulating the file format information based on at least one signal characteristic of the data object", as required by the independent claims, prior to "distributing a data object". Specifically, Allen does not disclose any form of key generation derived from manipulations of "file format information" or "signal characteristics" (Claims 25, 26).

The would be no need to descramble the data objects of the Applicants because none of the references scramble the said data objects to a predetermined signal quality level, and what follows, "logically associating a signal quality with a predetermined estimation of a bandwidth requirement for the session" (Claim 43). That the content of Hirose and Wasilewski et al.'s data is encrypted, it would not be possible to combine Allen's "content duplication" since the signal would be inaccessible as an inherent property of encryption. For at least this reason, the 103 rejections of Claims 24-26, 43, 45-47, and 50 (and the claims that depend therefrom) should be withdrawn.

§ 103 Rejections based on a combination of Hirose in view of Allen

Claim 61 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hirose (U.S. Patent No. 5,917,915) in view of Allen (U.S. Patent No. 5,418,713). Examiner asserts that "Hirose teaches all of the limitations of claim 60 above. However, Hirose does not teach the first data object comprises advertising. Allen teaches the first data object comprises advertising (col. 14, lines 31-44)," September 30, 2004 Office Action at Page 21. Applicants respectfully disagree. First, Hirose never mentions

bandwidth allocation based on linking between data objects. Additional arguments were previously presented above in connection with the Section 102 rejections. Specifically, Claim 60 teaches: "wherein a characteristic of the first data object causes a change in the second data object", Claim 61 depends from Claim 60. Arguments regarding Hirose, Allen and the two references in combination have been made above.

Second, where is the motivation to combine Hirose with Allen? As discussed in connection with Claims 24-26, 43, 45-47, and 50, above, Hirose's encrypted "newspaper data" cannot be linked in such a manner as to enable [emp[hasis added] "linking at least a first data object to at least one second data object; **wherein a characteristic** of the first data object causes a change in the second data object" rendering Allen's advertising useless. For these reasons, Applicants respectfully request the Section 103 rejections to be withdrawn.

Conclusion

Applicant maintains that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with Applicant's representative, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

Date: January 28, 2005

By: Scott A. Moskowitz

Scott A. Moskowitz
Tel# (305) 956-9041